

Information Technology Security Audit: A Study for Security and Challenges in Financial Sector in Nepal



Presenter: Suman Thapaliya, PhD Scholar
Department of Information Technology
Supervisor 1: Prof, Dr. Sateesh Kumar Ohja
Supervisor 2: Prof, Dr. Subarna Shakya

NPCERT to Host First Cyber Security Meetup in Nepal

**NEPAL
Cyber Security
Meetup #1**

**Thursday, 4th April 201
(2075 Chaitra 21)**

**Venue: Nepal Telecom Building
Babarmahal**

Organizer:
npcert
Information Security Response Team Nepal

Supported by:
ICT FRAME
ONE COVER
LWI
ICT Goal
Centre For Cyber Security Research and Innovation
BROADWAY
NATIONAL ICT COUNCIL



IT SECURITY AUDIT

WE SHOW YOUR PROBLEM

YOU SOLVE IT 😊

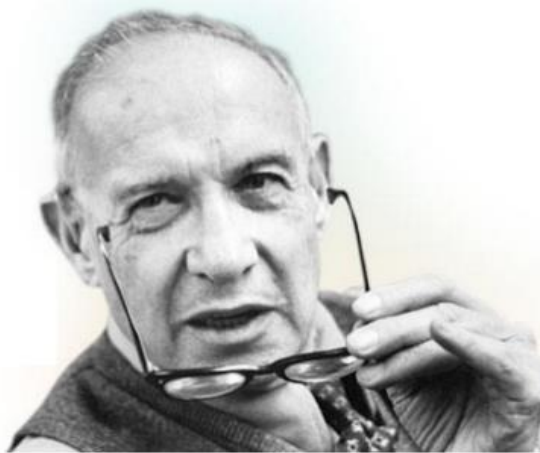
NPCERT to Host First Cyber Security Meetup in
Nepal

4/6/2019



AGENDAS

- INTRODUCTION
- PURPOSE
- MOTIVATION
- STATEMENT OF PROBLEM
- PROCESS
- FRAMEWORK
- RESEARCH METHODOLOGIES
- CASE STUDY
- RESULT & DISCUSSION
- CONCLUSION

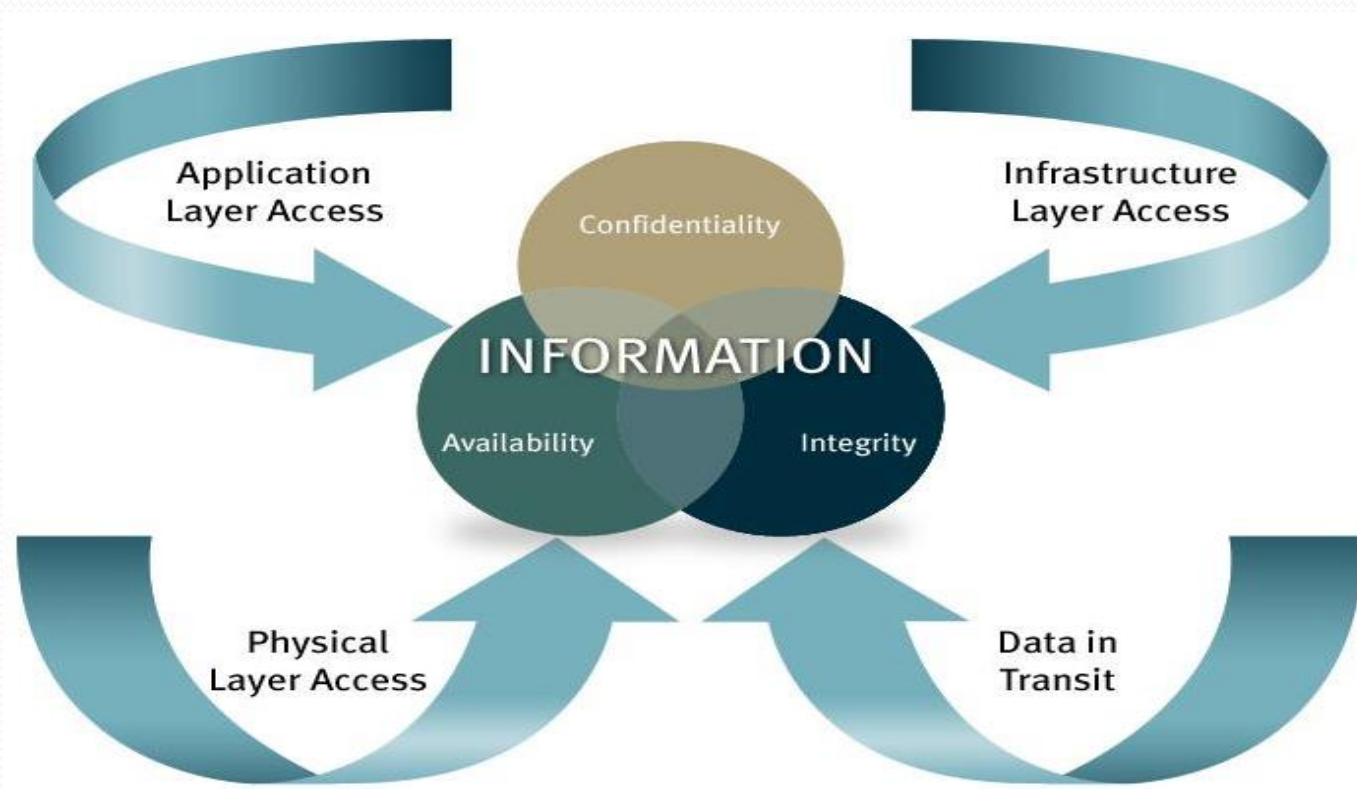


Peter Drucker

“There are:
Companies,
That make things happen
Companies,
That watch things happen
Companies,
That wonder what happened “



INTRODUCTION



Confidentiality: Is a set of rules that limits access to information.

Integrity: Is the assurance that the information is trustworthy and accurate.

Availability: Is a guarantee of reliable access to the information by authorized people.

NPCERT to Host First Cyber Security Meetup in
Nepal

INTRODUCTION

- When most people hear the word “audit,” their first reflex is to cringe. Usually, it means having some outside team come in to review everything and tell them what they’re doing wrong in technical term.
- An IT audit is the:
 1. Examination and evaluation of an organization’s information technology infrastructure.
 2. Policies and operations.

Information technology audits determine:

1. Whether IT controls protect corporate assets
2. Ensure data integrity and are aligned with the business’s overall goals.

IT auditors examine not only physical security controls, but also overall business and financial controls that involve information technology systems.

WHY TO AUDIT

- Company knows only after attack
- Are client/ customer safe to invest ?
 - Invest Data
 - Invest Information
 - Invest Money
 - Invest Career and so on.
- Are promoter and shareholder safe ?
- What will be the loss value ?
- When will you recover ?
- What sort of Disaster you may face ?

CYBER ATTACK

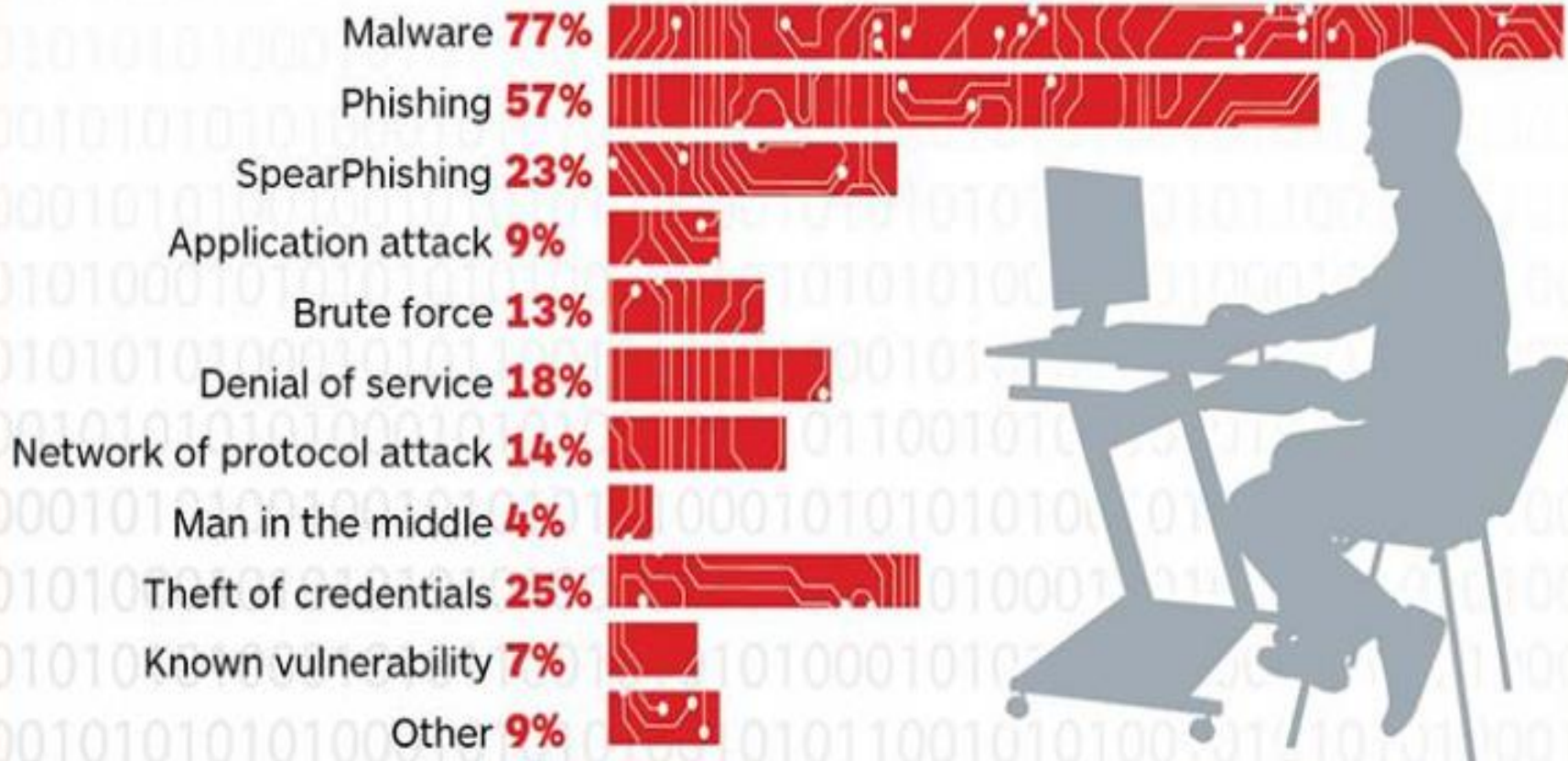
- Story Time 😊

Global Risks Report		North America
		The risks of greatest concern for doing business
		rank
Cyber attacks		1
Terrorist attacks		2
Asset bubble		3
Fiscal crises		4
Failure of climate change adaptation		5

Source: Executive Opinion Survey 2017, World Economic Forum

PAST ATTACK NATURE

What was the nature of the attack?



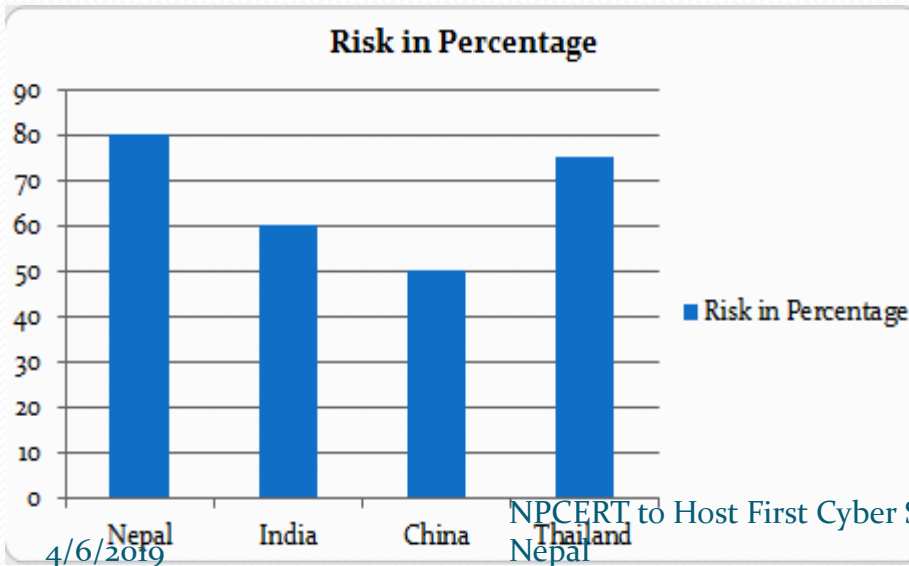
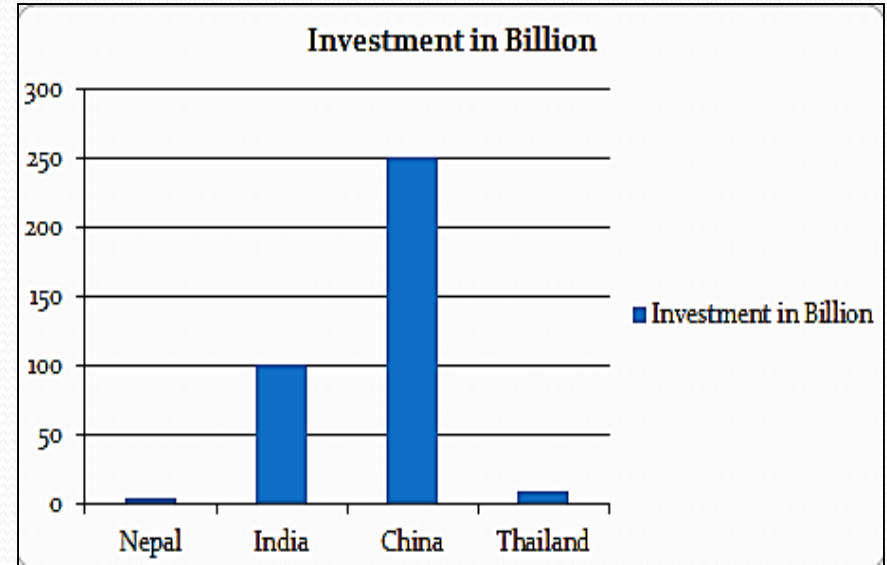
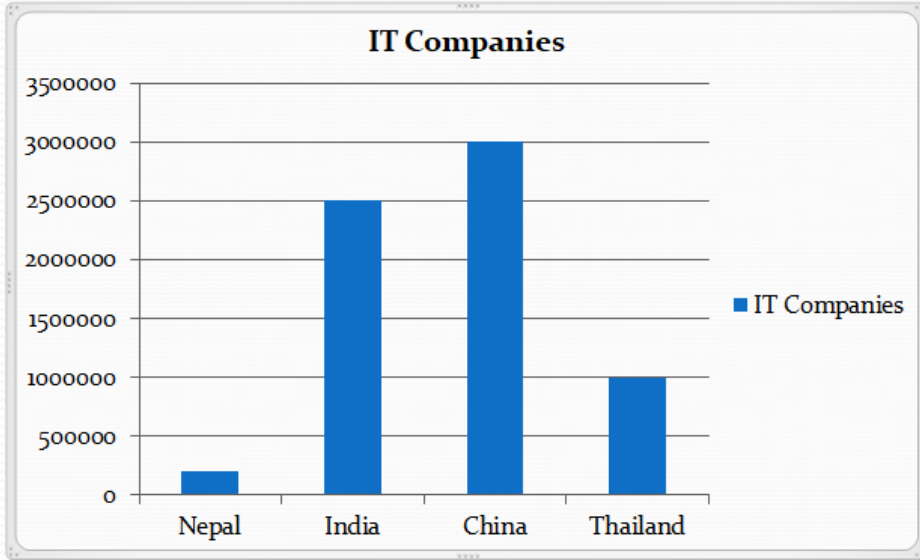
PURPOSE

- The purposes of an IT audit are to evaluate the system's internal control design and effectiveness.
- This includes, but is not limited to, efficiency and security protocols, development processes, and IT governance or oversight.

STATEMENT OF PROBLEM

- Many organizations are spending large amounts of money on IT because they recognize the tremendous benefits that IT can bring to their operations and services. However, they need to ensure that their IT systems are reliable, secure and not vulnerable to computer attacks.
- Introduction of New Threats and Attack are you updated ?
- Assurance of IT system adequately protected
- Less knowledge on IT
- Not providing importance to data
- Continuous loss of data and hacked

PROBLEM STATEMENT – Practical Gap



Less Investment , High Risk

SOLUTION

- To give assurance that IT systems are adequately protected.
- Provide reliable information to user and properly managed to achieve their intended benefits.
- Reduce Risk of data tampering
- Reduce Data loss or leakage
- Reduce Service disruption
- Provide Proper management of IT System

MOTIVATION

Different kinds of cyber attacks that are mostly transpired in Nepal. List of those cyber attacks are as mentioned:

- Attacks on social media
- Piracy
- Identity Threat
- Unauthorized access
- Website hacking



HOME

NEWS

EVENTS

STARTUPS

INTERVIEW

AUTO LIFE

HEALTH & SCIENCE

SECURITY

Home > Security > Nepal in high risk of cyber attacks

Security

Nepal in high risk of cyber attacks



NPCERT to Host First Cyber Security Meetup in Nepal

CASE STUDY 1

1. Pune Citibank Mphasis Call Center Fraud
some ex employees of BPO arm of Mphasis Ltd Msource, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection".

The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

CASE STUDY 2

WannaCry

- The most infamous ransomware attack of 2017 was a strain of ransomware called WannaCry that spread all over the globe.
- The ransomware targeted numerous public utilities and large corporations, most notably National Health Service hospitals and facilities in the United Kingdom, hobbling emergency rooms, delaying vital medical procedures, and creating chaos for many British patients.
- Though the origin of WannaCry is not yet known, the US government has **blamed** the Kim Jong-un-led North Korean government for initiating the attack

CASE STUDY 3

3. The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the bank's computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

CASE 4: Attacks in 2017

- Petya/NotPetya: Affected Across the globe in 2017, spread in computers, pharmaceutical company merck, danish shipping company, Russian oil giant rosneft, power companies in Ukrainian, airports, public transit and country's central bank.
- Zomato hack: zomato, largest restaurant aggregators in India was hacked and some of its user accounts were being sold on the dark web.
- The HBO Hack: Revealed script for Episode 4 of season 7 of Game of Thrones, which was scheduled to be released the following week, was put up online for the whole world to see.
- Equifax: In July, a group of hacker penetrated Equifax, one of the largest credit bureaus in the worlds and stole personal data of 145 million people.

Top Attack

1. Adobe was going through hell: 2.9 million accounts was stolen.
2. Panic to sony: Personal data of 77 million users which was leaked to public.
3. The south Korean Nightmare: Data from 100 million credit cards had been stolen.
4. Target Targeted: Data from 110 million customers was hijacked, including 40 million customers and personal data.
5. Adult Friend Finder exposed: Dating site was attacked, 4 million accounts was made public.
6. Marriott Hotels: Privacy of 500 million customers compromised, including banking data.
7. Theft of more than 1 billion passwords: Russian hackers stole 1.2 billion logins and passwords on 420000 websites.

Nepal Bank Got Hacked 😞

Report: Attackers Hacked Nepalese Bank's SWIFT Server

\$4.4 Million Moved to Accounts in US, UK and Japan via Fraudulent SWIFT Messages

Nepal recovers 'most' of the money hacked from bank

Nepal bank latest victim in cyber heists, recovers most of the funds

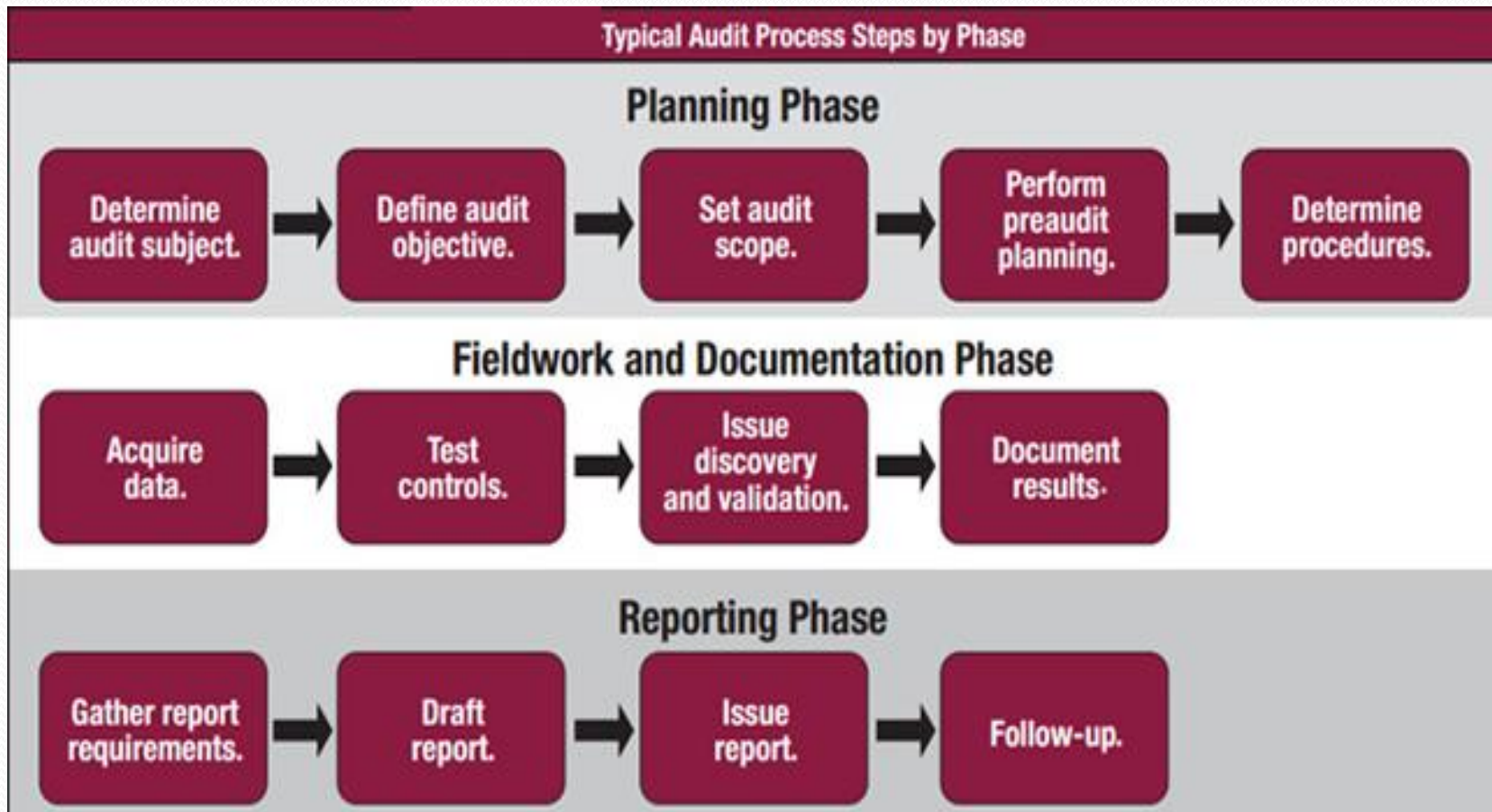
Nepal Faced Around 800 Cyber Attacks Last Year

IS Risk Measure/ Level

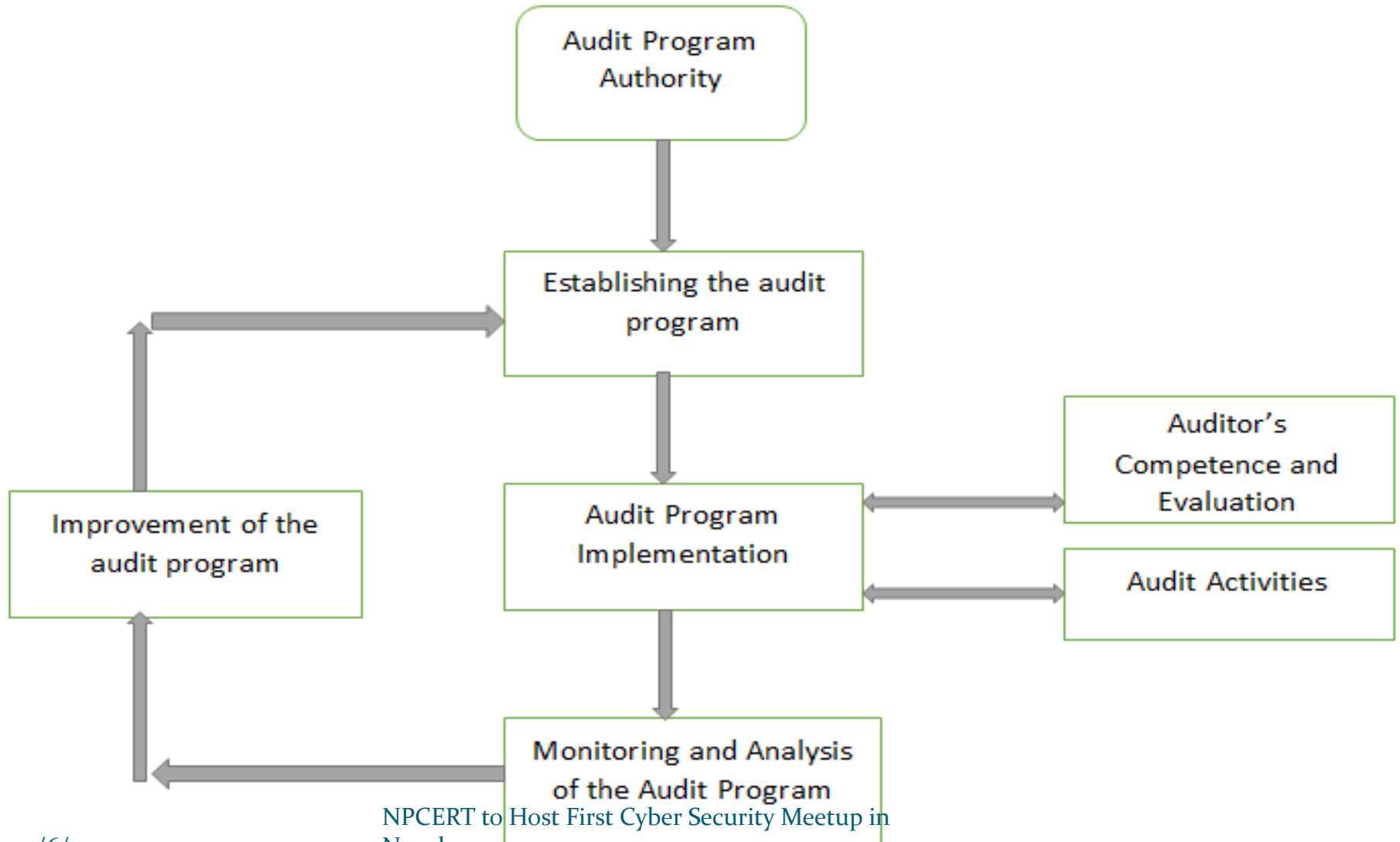
INFORMATION SECURITY RISK RATING SCALE	
EXTREME (13 – 15)	Extreme risk of security controls being compromised with the possibility of catastrophic financial losses occurring as a result. (HUGE LOSS)
HIGH (10 – 12)	High risk of security controls being compromised with the potential for significant financial losses occurring as a result. (MID LEVEL LOSS)
ELEVATED (7 – 9)	Elevated risk of security controls being compromised with the potential for material financial losses occurring as a result. (MINOR LOSS)
MODERATE (4 – 6)	Moderate risk of security controls being compromised with the possibility of limited financial losses occurring as a result. (COMPROMISE LOSS)
LOW (1 – 3)	Low risk of security controls being compromised with measurable negative impacts as Loss. (NEGATIVE IMPACT)

IT Audit Process

- The below provided are the basic steps in performing the Information Technology Audit Process.



Audit Program Management Process Flow

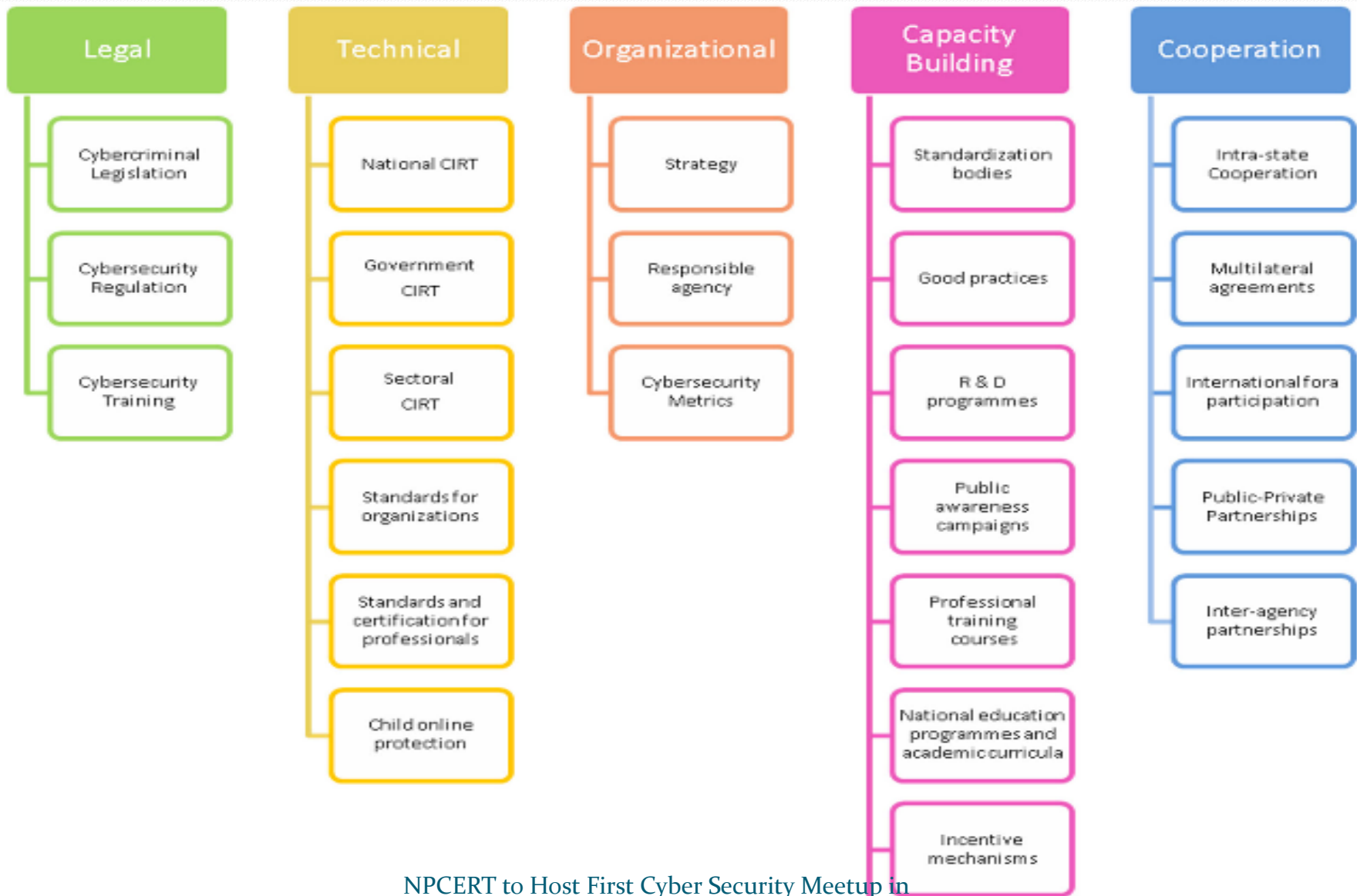


Conceptual Framework

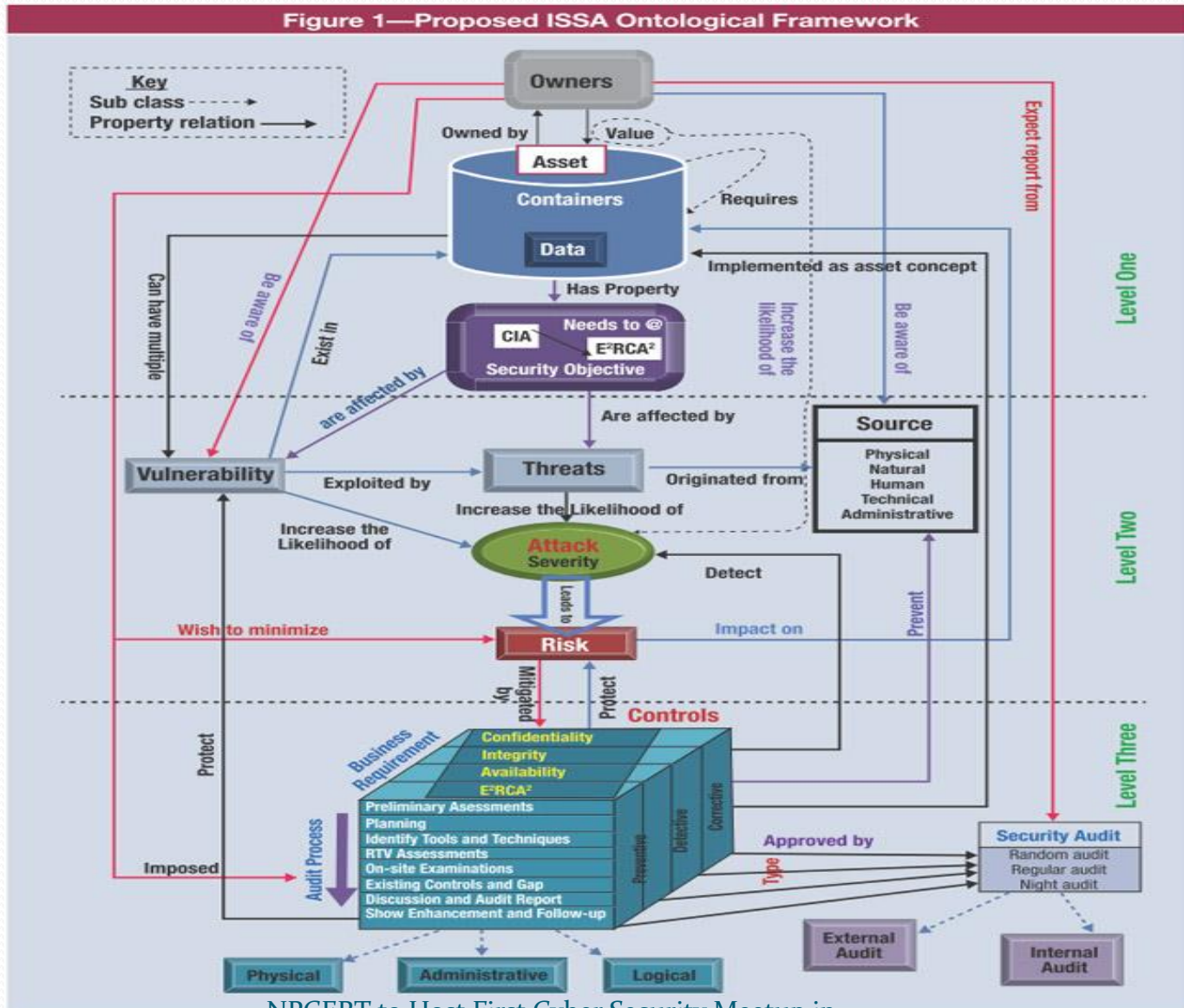
The five pillars are briefly explained below:

- **Legal:** Measured based on the existence of legal institutions and frameworks dealing with cyber security and cybercrime.
- **Technical:** Measured based on the existence of technical institutions and frameworks dealing with cyber security.
- **Organizational:** Measured based on the existence of policy coordination institutions and strategies for cyber security development at the national level.
- **Capacity Building:** Measured based on the existence of research and development, education and training programme; certified professionals and public sector agencies fostering capacity building.
- **Cooperation:** Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Pillars and Sub Pillars



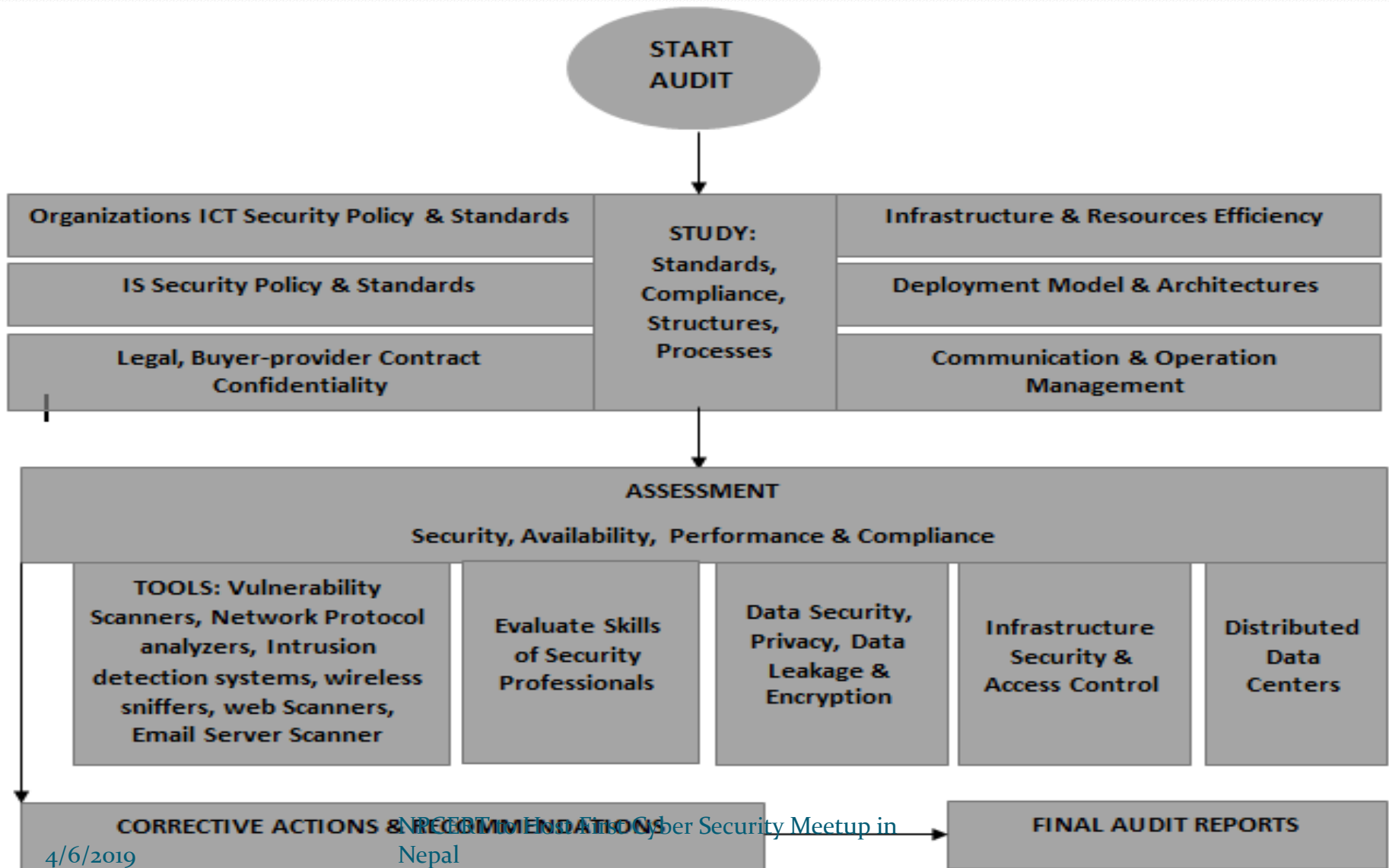
Final Prototype



Source: S. G. Kassa. Reprinted with permission.

NPCERT to Host First Cyber Security Meetup in Nepal

Simplified Audit Process



Framework Components Defined

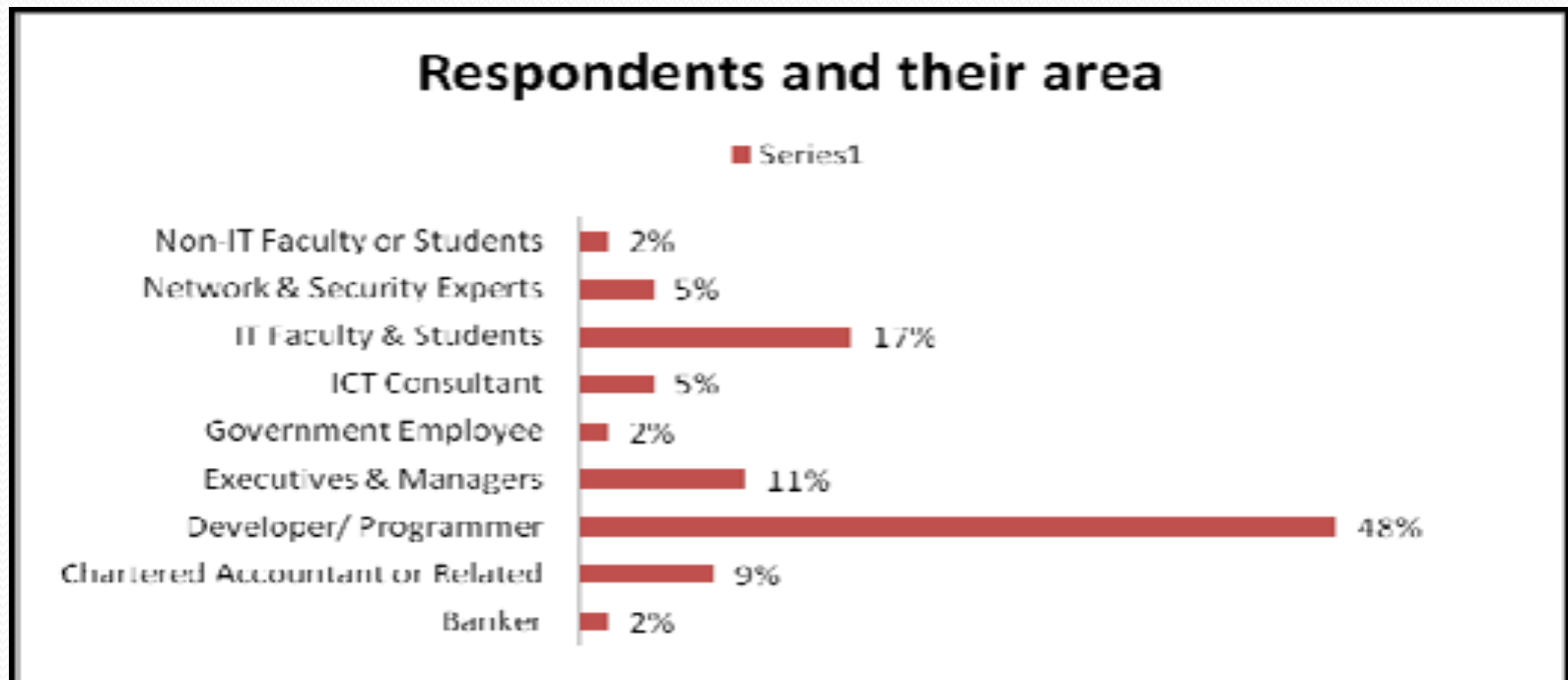
- **Owner:** The person or entity that has been given formal responsibility for the security.
- **Asset:** Any tangible or intangible resource that has value to the owner of the organization or entity.
- **Data:** A collection of all financial and nonfinancial facts, records and information.
- **Containers:** the place where an information asset or data “lives” or any type of information asset (data) is stored.
- **Security Objective:** A Statement of intent to counter specified threads and/or satisfy specified organizational security policies or assumptions.
- **Vulnerability:** A flaw or weakness of an asset or group of assets that can be exploited by one or more threats.
- **Threat:** An unwanted incident that may result in harm to a system or organization.
- **Sources:** Either intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.
- **Attack:** Any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- **Severity:** The level of harm that may occur as a result or exposure to or contact with a hazard.
- **Risk:** The likelihood of harm occurring, combined with the potential severity of an event, to produce a level of risk or risk rating.
- **Audit process:** A step-by-step procedure to achieve the security objective of an asset.

METHODOLOGY

- Quantitative Research Methodology has been used in this research. The research theory of this paper has been to construct knowledge and meaning from Researchers experience, that is, Constructivism, which has direct application to education. The research theory indicates technological Constructivism.
- Primary data were collected by means of online survey, Questionnaire and Interview where professionals from different areas of ICT were chosen, which helped to study current situation in Nepal. Secondary data were collected from several comparative studies of different research papers/ journals, websites, newspaper which helped to gather information on international level.

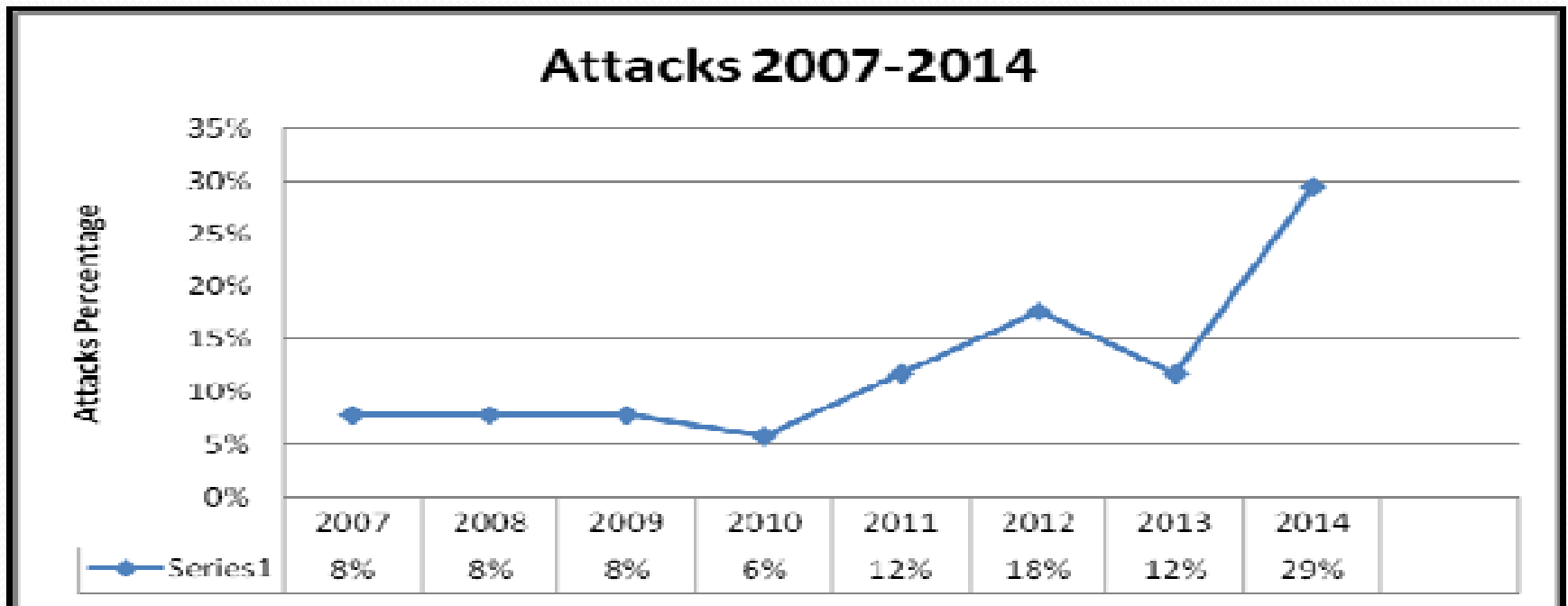
RESULT & DISCUSSION

- A survey was conducted to support this research and different charts are presented for further clarifications. There were 108 respondents to qualify in Fig.

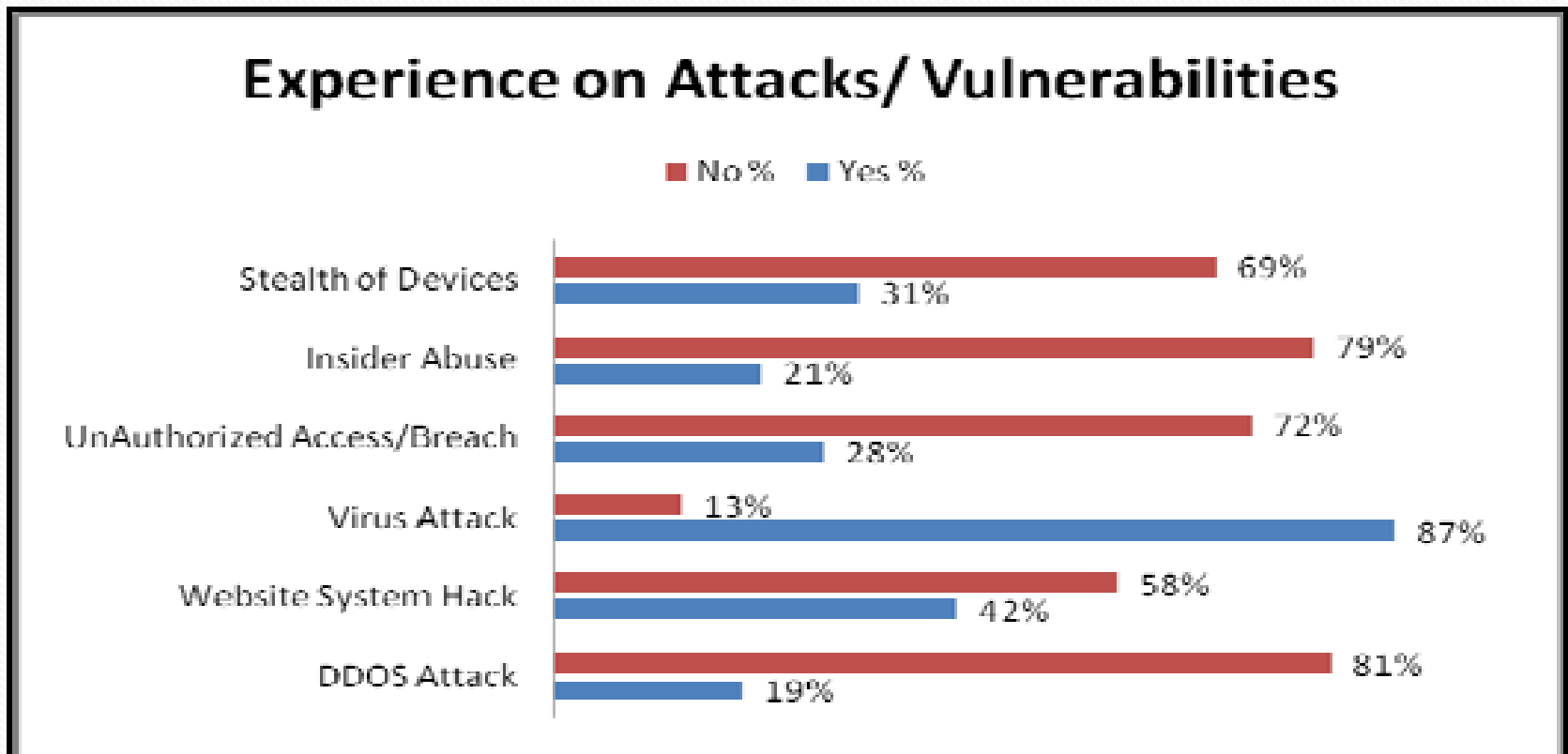


RESULT & DISCUSSION Cont ...

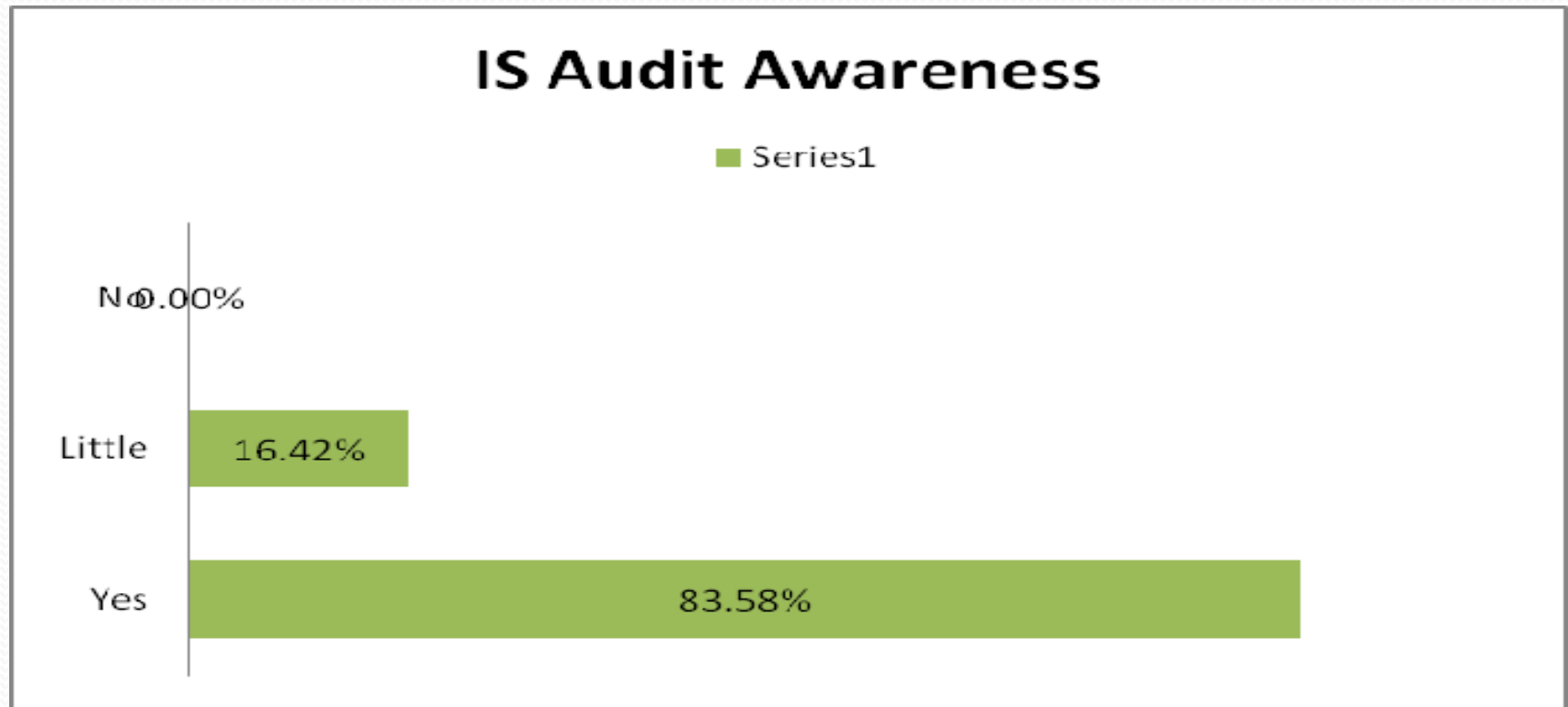
- Shows attacks from 2007 to 2014 has been growing relatively with prominent probability of attacks in any components of security audit mentioned in Fig.



- Depicts experience on the different types of attacks or vulnerabilities experienced by user from 2007-2014 by ICT users from different fields as in Fig.



- Depicts IS Audit Awareness in Nepal by 83.58% which looks promising as IS Audit practicing would not be very difficult job to begin.



CONCLUSION

Information Security is an increasingly important part of our life today, and the degree of interconnectivity of

- Networks implies that anything and everything can be exposed, and everything from national critical
- Infrastructure to our basic human rights can be compromised. Governments are therefore urged to
- Consider policies that support continued growth in technology sophistication, access and security, and as a crucial first step, to adopt a national cyber security strategy.
- Risk assessment and security audit has to be conducted eventually to minimize and mitigate risks. Local law, local and international standards and policy must be followed while preparing the ICT Security policies in an organization. Audit is must for data security assurance. This research has proposed an audit model for IS Audit which is highly recommended for IS Audit in any IS Audit and Security Vulnerability minimizing.



4/6/2019

NPCERT to Host First Cyber Security Meetup in Nepal